Department of Homeland Security IAIP Directorate Daily Open Source Infrastructure Report for 13 June 2005

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- Netcraft reports that smaller banks and credit unions involved in acquisitions have been increasingly targeted by phishing attacks in the last several months, as small banks have been less active in educating customers on this topic than the huge banks that were the primary targets in early phishing scams. (See item 5)

- The New York Times reports that the Agriculture Department said Saturday it would conduct further tests on an animal suspected of having mad cow disease before confirming the results. (See item 10)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base

Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping

Sustenance and Health: Agriculture; Food; Water; Public Health

Federal and State: Government; Emergency Services

IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard

Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS/IAIP Products &Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 10, Department of Energy* — **Bodman announces Strategic Petroleum Reserve fill to be complete in August.** Secretary of Energy Samuel Bodman announced on Friday, June 10, that the planned fill of the Strategic Petroleum Reserve (SPR) will be complete in August, when the SPR reaches 700 million barrels of oil. President Bush directed the fill in November 2001 as a means to strengthen the nation's energy security in the wake of the 9/11 terrorist attacks. When the fill is complete, the President’s decision will have added approximately 159 million barrels of crude oil to the nation’s emergency stockpile. "Taking steps to prepare for a severe disruption in the oil markets is vital to our economic and national security. By filling the

Strategic Petroleum Reserve to its highest level in history, American consumers and businesses are more protected today in the event of a major disruption in our oil supplies, whatever the cause," said Bodman. The Strategic Petroleum Reserve is the world's largest inventory of emergency crude oil, which is stored in deep underground caverns in salt formations along the Texas and Louisiana Gulf Coast. In the event of a severe oil supply disruption, the SPR can be called upon to protect U.S. consumers from economic harm, and to provide fuel for national defense.
Additional information about the SPR: http://fossil.energy.gov/programs/reserves/index.html
Source: http://www.energy.gov/engine/content.do?PUBLIC_ID=18039&BT_CODE=PR_PRESSRELEASES&TT_CODE=PRESSRELEASE

2. *June 09, Nuclear Regulatory Commission* — **Nuclear Regulatory Commission restoring more documents to online library.** The Nuclear Regulatory Commission (NRC) is restoring public access to more than 70,000 additional documents through its online public library, ADAMS, after reviewing them for security sensitivity. The restoration involves administrative, contractual, research and other documents not related to specific licensees that were deemed non−sensitive as a result of the NRC's review. The documents were removed from the ADAMS library on October 25, 2004, along with hundreds of thousands of others, to conduct a security review and remove information that could potentially be of use to a terrorist. The NRC remains committed to operating as an open agency and conducting its business in public to the extent possible. The agency has already restored access to about 163,000 non−sensitive documents in several categories, including those pertaining to reactors, Yucca Mountain and selected hearings. Most documents dealing with nuclear materials (i.e., non−reactor) licensee documents have not been restored, and the Commission continues to evaluate them. It is expected that the restoration process for the 70,000 documents will be completed by June 20.
The newly restored documents will be available through the Electronic Reading Room on the NRC Website at http://www.nrc.gov.
Source: http://www.nrc.gov/reading−rm/doc−collections/news/2005/05−0 90.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.

[Return to top]

Defense Industrial Base Sector

3. *June 10, Associated Press* — **Evacuation ends after Navy checks out tampered locks on railcar.** A tampered lock on a railroad car carrying a U.S. Navy rocket motor prompted the evacuation of about 100 people living near Yermo, CA, on Friday, June 10. The voluntary evacuation that began shortly before 2:30 a.m. ended 7½ hours later, after the load was inspected and no damage was found and the car was relocked, said John Bromley, a spokesperson for Union Pacific. The railcar contained a first−stage rocket motor for a Trident D5 missile, according to a statement from the China Lake Naval Weapons Station. Union Pacific notified San Bernardino County sheriff's deputies about a burglar alarm on the car at

2:20 a.m., sheriff's spokesperson Chip Patterson said. "Deputies responded and they discovered some bolts to the boxcar had in some way been tampered with and it had been opened," Patterson said. The Navy sent an explosive ordnance disposal team to the site to check out the motor and the environmentally controlled railcar. There was no apparent danger to the community, the China Lake statement said.
Source: http://www.signonsandiego.com/news/state/20050610−1550−ca−desertevacuation.html

[Return to top]

Banking and Finance Sector

4. *June 10, Voice of America* — **Experts say progress made in fighting terrorist financing.** International experts say progress has been made to curb money laundering and terrorism financing, but more needs to be done. Officials from the Financial Action Task Force (FATF), an inter−governmental body monitoring efforts against money laundering and the financing of terrorism, say criminals continue to find loopholes in the international financial system to move illegal funds. At the end of a three day conference organized by FATF in Singapore, FATF president Jean−Louis Fort said governments must step up efforts to make it difficult for money launderers and terrorists to move money around. FATF officials stressed the importance of more effective monitoring of cash couriers and underground remittance systems, unregulated methods of transferring money from country to country. This issue remains a challenge particularly in Asia, where there are huge populations of migrant workers remitting money to their homeland. Officials call for continued monitoring of the hawala remittance system common in South Asia and the Middle East −− a traditional network of remittance agents that leaves a sparse or confusing paper trail.
Financial Action Task Force: http://www.fatf−gafi.org
Source: http://www.voanews.com/english/2005−06−10−voa20.cfm

5. *June 09, Netcraft* — **Bank mergers provide opportunity for phishing.** Scammers are using bank mergers as an opportunity to craft customized phishing scams timed to transitions between the banks' online systems, hoping that customer awareness of mergers will bring more takers on phishing e−mails. The wide adoption of online banking means that most industry mergers will include a consolidation of IT systems and customer accounts, offering phishing crews a steady supply of migration scenarios to target. There were about 1,500 bank mergers per year in the U.S. between 1996 and 2002, according to the Federal Reserve. While headlines have focused on megamergers between industry giants, much of the acquisition activity involves growing regional and local banks. These smaller banks and credit unions have been increasingly targeted by phishing attacks in the last several months, as phishers adapt their strategies to seek easier prey. While consumer education about phishing has been a priority for the entire U.S. banking industry, small banks have been less active in this regard than the huge banks that were the primary targets in early phishing scams.
Source: http://news.netcraft.com/archives/2005/06/09/bank_mergers_provide_opportunity_for_phishing.html

[Return to top]

Transportation and Border Security Sector

6. *June 10, Associated Press* — **Alaska Airlines passengers experiencing more delays and cancellations.** Alaska Airlines passengers are experiencing more delayed flights and cancellations, the airline acknowledges. It's been that way for months, company spokesperson Caroline Boren said. "We're trying to find out exactly what the problems are," she added. One reason is because planes are being targeted for maintenance by flight crews more often, and maintenance is taking longer, she said. The situation was exacerbated Sunday, June 4, when the airline added 59 flights to reach its summer schedule of 517 flights per day. Company spokesperson Amanda Tobin said the schedule change — not labor issues with baggage handling — seemed to cause extra delays.
Source: http://www.usatoday.com/travel/flights/2005−06−10−alaska−del ays_x.htm

7. *June 10, Bloomberg News* — **Acela service to return to East Coast in July.** Amtrak next month will resume Acela high−speed train service, which was suspended in April because of brake problems, the railroad's chief of operations said Thursday, June 9. The return will be gradual, with all 20 Acela trains back in service in the fall after repairs are made, William L. Crosbie said at a House Transportation Committee hearing in Washington. He didn't give a specific month. The trains, which can reach 150 miles an hour, serve New York, Washington and Boston, and account for more than 20 percent of Amtrak's ticket sales. Amtrak has said the suspension of Acela service has cost it about $1 million a week. The trains were taken out of service April 15 after inspectors found cracks in about 20 percent of brake rotors. The railroad is testing a new type of rotor to replace the cracked ones, Crosbie said. The replacements change the rotor design to reduce vibrations when the brakes are applied, said R. Clifford Black, an Amtrak spokesperson. The vibrations may have caused the cracks, Black said.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2005/06 /09/AR2005060901707.html

8. *June 10, San Antonio Express−News* — **Tractor−trailer carrying explosives overturns in San Antonio.** An 18−wheeler carrying high explosives rolled over Friday morning, June 10, on Interstate 35 in the Windcrest area of Northeast San Antonio, TX. The truck driver was northbound on Interstate 35 and taking the exit to Loop 410 West when the accident occurred on the hairpin turn. I−35 was shut down in both directions near the Loop 410 exit. Authorities evacuated businesses and residences within a half−mile of the accident scene. Fire Department spokesperson Randy Jenkins said the truck was carrying 3,000 pounds of shaped charge material used to initiate explosives. "We don't feel that citizens need to worry about an explosion, but we did evacuate the area," Jenkins said. The Police Department bomb squad and a Fire Department hazardous materials team responded to the accident. An elderly care center near the scene was evacuated to nearby schools.
Source: http://www.mysanantonio.com/news/metro/stories/MYSA061005.ro llover.en.2fddbf0fc.html

[Return to top]

Postal and Shipping Sector

Nothing to report.
[Return to top]

Agriculture Sector

9. *June 12, Chicago Tribune (IL)* — **Mad cow disease found in U.S. beef cow.** An American beef cow has tested positive for mad cow disease, and additional tests will have to be done at a British laboratory to confirm the results, Agriculture Secretary Mike Johanns said Friday, June 10. The meat of the animal that tested positive did not get into the nation's food chain, Johanns said. If the British lab concurs with the test result, it would be the nation's second confirmed case of mad cow disease, known technically as bovine spongiform encephalopathy. The first case was found in December 2003 in Washington state in a dairy cow that had been fed in Canada. Agriculture Department officials said they did not yet know which state the cow came from.
Source: http://www.chicagotribune.com/news/nationworld/chi−050612020 0jun12,1,3231906.story?coll=chi−newsnationworld−hed

10. *June 11, New York Times* — **More tests planned in suspected case of mad cow disease.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns confirmed Friday, June 10, that an older animal had tested positive for mad cow disease. Officials from the USDA said Saturday that a series of tests would be carried out on the cow's brain tissue at a department laboratory in Ames, IA, and at an internationally known facility in Weybridge, Britain, to determine if the animal is infected with mad cow disease, the the brain−wasting disease clinically known as bovine spongiform encephalopathy. Confirmation that the animal had mad cow would make it more difficult for Johanns to reopen the border to live cattle from Canada, which he has said is a top priority. The United States closed the border after mad cow disease was discovered in a Canadian cow in May 2003. Two additional cases were confirmed in Canada last year. The only confirmed case of mad cow in the United States−−found in December 2003 in a Washington State dairy cow that was born in Alberta−−dealt a huge blow to the nation's $90 billion beef industry.
Source: http://reuters.myway.com/article/20050611/2005−06−11T081503Z _01_N11684938_RTRIDST_0_NEWS−MADCOW−USA−DC.html

[Return to top]

Food Sector

11. *June 09, Food Safety and Inspection Service* — **Ground beef products recalled.** Murry’s, Inc., a Lebanon, PA, firm, is voluntarily recalling approximately 63,850 pounds of frozen ground beef products that may be contaminated with E. coli O157:H7. The recall was prompted by epidemiological evidence provided to Food Safety and Inspection Service by the state of New Jersey related to an illness linked to consumption of this product. E. coli O157:H7 is a potentially deadly bacteria that can cause bloody diarrhea and dehydration. The very young, seniors, and persons with compromised immune systems are the most susceptible to foodborne illness.
Source: http://www.fsis.usda.gov/News_&_Events/Recall_026_2005_Relea se/index.asp

12. *June 08, Food and Drug Administration* — **Pet food recalled.** T.W. Enterprises of Ferndale, WA, Thursday, June 9, alerted consumers that it is recalling certain dog and cat treats it markets because they may be contaminated with Salmonella Thompson. People handling these treats can become infected with Salmonella Thompson, especially if they have not thoroughly washed their hands after having contact with any the treats or any surfaces exposed to these products. Salmonella Thompson is an organism which can cause serious infections in small children, frail, or elderly people, and others with weakened immune systems. Healthy people may only suffer short−term symptoms, such as high fever, severe headache, vomiting, nausea, abdominal pain, and diarrhea. Long term complications can include arthritis. T.W. Enterprises Inc. manufactured these pet treats and distributed them throughout the U.S. under its name and the Aron Pet Food name. The Food and Drug Administration became aware of the problem after five cases (three in Canada and two in the U.S.) of Salmonella Thompson infection developed among people who may have handled these pet treats. Follow up analysis indicated that the illnesses were linked to these pet treats.
Source: http://www.fda.gov/oc/po/firmrecalls/tw06_05.html

[Return to top]

Water Sector

13. *June 09, Los Angeles Times* — **Water safety tops EPA chief's list.** Environmental Protection Agency (EPA) Administrator Stephen L. Johnson predicted Wednesday, June 8, that safeguarding the country's water supply — from terrorists and pollutants — would be one of the pressing environmental concerns of the 21st century. "I believe water, over the next decade and further, will be the environmental issue that we as a nation and, frankly, as a world will be facing," he said. Keeping the nation's water safe and secure is "an area of vulnerability for the United States and also an opportunity for us." Johnson, the first scientist to head the EPA, said in addition to helping the Department of Homeland Security protect the water supply, he wanted to find economically viable solutions for the 10% of Americans whose drinking water was not healthy. He also spoke of helping cities and municipalities improve aging water treatment facilities.
Source: http://www.latimes.com/news/nationworld/nation/la−na−epa9jun09,1,3499044.story?coll=la−headlines−nation

[Return to top]

Public Health Sector

14. *June 12, AFX News* — **Hundreds diagnosed with hepatitis in Russia.** Some 461 people have been hospitalized in a Hepatitis A outbreak in southwest Russia's Tver region. The outbreak is believed to have been caused by a local beer, produced by the Rjevpivo brewery. "It is expected that for another few days, about 40 people will contract the disease daily, and then the number will start to decline," Tver Governor Dmitry Zelenin told reporters. Officials said earlier that the newly hospitalized were in better condition than those who fell ill a few days before, in an indication that the illness is now being diagnosed in its early stages. A number of cases have

also been recorded in Moscow and the western province of Smolensk. Hepatitis A is a highly contagious viral infection of the liver.
Source: http://www.interfax.ru/e/B/politics/28.html?id_issue=1131003 9

15. *June 11, New York Times* — **Flu outbreaks in China raise fears of a mutant virus.** Two new outbreaks of avian flu among birds in western China have raised fears that the virus is being spread widely by migrating birds and mutating rapidly. The regional director for the World Health Organization, Shigeru Omi, told reporters Friday, June 10, that the two recent outbreaks in remote areas in which hundreds of birds died were worrisome because they involved migratory waterfowl and domestic geese, birds that until now had been fairly resistant to the disease. More than 13,000 geese were destroyed in Tacheng, in the Xinjiang autonomous region, after about 500 died of H5N1 avian flu, China's Agriculture Ministry reported. Previously, the H5N1 flu had been lethal to domestic chicken flocks, but veterinary officials had believed that geese and wild birds carried the disease without dying of it.
Source: http://www.nytimes.com/2005/06/11/health/11flu.html

16. *June 10, Food and Drug Administration* — **FDA approves a new whooping cough vaccine.** The Food and Drug Administration (FDA) Friday, June 10, approved a new vaccine for a single booster immunization against pertussis (whooping cough), in combination with tetanus and diphtheria, for adolescents and adults 11−64 years of age. The vaccine will be marketed as Adacel by Aventis Pasteur Limited located in Toronto, Canada. Adacel is the first vaccine approved as a pertussis booster for adults. Vaccines for prevention of tetanus and diphtheria (Td vaccine) in adolescents and adults have been available for many years. Recently, FDA approved a similar vaccine called Boostrix, manufactured by GlaxoSmithKline, for use in adolescents 10−18 years of age. Pertussis is a highly communicable and potentially serious illness in adolescents and adults. In young infants, pertussis is more frequently severe and can be fatal, particularly in those too young to be fully vaccinated. Since 1980, the rates of reported pertussis cases have been increasing in adolescents and adults, as well as in young infants. Adolescents and adults have been implicated as the source of pertussis infection for susceptible young infants, and other family members.
Source: http://www.fda.gov/bbs/topics/ANSWERS/2005/ANS01361.html

17. *June 10, New York Times* — **Fungus may aid global war on malaria.** In a finding that may open promising new ways to attack malaria, scientists are reporting that two fungi that are harmless to humans and the environment can be used to kill mosquitoes. The fungi are already licensed in Western countries to control aphids, termites, and other pests. One of the researchers, Matt Thomas, a biologist at Imperial College in England, estimated that a "deliverable product" could be ready in three to five years. Malaria kills more than one million people a year. Yeya Touré, chief of insect research for the World Health Organization's malaria branch, called the studies "quite promising," but added that he wanted to see more tests of safety and effectiveness −− in particular, how long the fungi would remain lethal when sprayed on walls or soaked into mosquito nets.
Source: http://www.nytimes.com/2005/06/10/science/10mosquito.html?or ef=login

18. *June 09, University of Houston* — **New biosensor technology.** A University of Houston student has made a breakthrough in biosensors that could help bioterrorism researchers in their ability to quickly and accurately detect toxic biological agents. Mrinal Shah, a doctoral student

in chemical engineering at the University of Houston, has developed new methods in the use of biosensors that could provide one of the first steps in developing a protein−based biosensor that would help the government in safeguarding the nation. Shah employs liquid−liquid phase separation −– a technique that is similar to the concept behind how oil and water separate. His research makes use of the proteins needed in biosensors and accurately controls the nucleation of those proteins. “The development of a successful biosensing chip has potential uses that are manifold and urgently needed with several applications that are immediately significant,” Shah said. “If there is biological warfare somewhere, and you put this chip into that environment, you would know exactly what is in that environment, and safety precautions could be taken. That’s the ultimate achievement that every scientist working in protein chips dreams about.”
Source: http://www.uh.edu/admin/media/nr/2005/06june/060905biotoxica gnts.html

19. *June 09, Rockefeller University* — **Researchers create infectious hepatitis C virus in a test tube.** A team of researchers led by scientists at The Rockefeller University has produced for the first time an infectious form of the hepatitis C virus (HCV) in laboratory cultures of human cells. The finding will allow scientists to study every stage of the HCV life cycle and develop drugs to treat this life−threatening disease that affects more than 170 million people around the world. "The inability to reproduce aspects of the hepatitis C virus life cycle in cell culture has slowed research progress on this important human pathogen," says senior author Charles Rice, head of the Laboratory of Virology and Infectious Disease at Rockefeller. "This system lays the foundation for future test tube studies of the virus life cycle and may help in the development of new drugs for combating HCV," adds Rice. Like all viruses, HCV cannot replicate by itself; instead it takes over the machinery of a host cell to make copies of itself. Much about the life cycle of HCV remains poorly understood because scientists have been unable to reproduce an infectious form of HCV that they can observe in cell cultures. The method developed by Rice and his colleagues changes that.
Source: http://www.rockefeller.edu/pubinfo/060905b.php

[Return to top]

Government Sector

Nothing to report.

[Return to top]

Emergency Services Sector

20. *June 11, The News−Gazette (IL)* — **Fire teams test rescue skills in mock tornado drill.** Ten teams of rescue specialists from throughout Illinois were pulled together in a continuous 33−hour mock tornado drill in Champaign. Under the scenario, "people" were trapped or crushed in buildings. Rescue workers pulled out 98 casualties during the two−day drill at the Illinois Fire Service Institute. The drill tested the skills of technical rescue teams from fire departments throughout the state. The "damage" portrayed at the various stations made it necessary for rescue workers to proceed carefully to prevent any further "collapse" or injury. Each of ten technical rescue teams went through six stations, testing their ability to rescue or retrieve victims of collapsed structures. They worked in three−hour shifts, got a 45−minute

break and then went on to each of the six stations, said Dan Smith, Region 7 coordinator for the Illinois Emergency Management Association. Part of the exercise was to test the deployability and skills of the technical rescue teams. Included in that test was whether a team is able to be self−sufficient for up to 24 hours, he said.
Source: http://www.news−gazette.com/localnews/story.cfm?Number=18398

21. *June 10, University of Scranton (PA)* — **Pennsylvania university establishes a homeland security institute.** This week in northeastern Pennsylvania, The University of Scranton announced the establishment of a Homeland Security Institute to engage in applied research related to regional and national security issues and to educate and train homeland security professionals and emergency response personnel. The Homeland Security Institute is one of only six institutions in Pennsylvania that is a member of the National Academic Consortium of Homeland Security based at Ohio State University, comprised of public and private institutions engaged in scientific research, education and training, and service programs aimed at identifying solutions to issues related to national security. The institute will be housed in the Graduate School of The University of Scranton and will develop and submit research proposals involving applications and solutions to problems that threaten regional and national security. The institute will provide training to area professionals regarding homeland security and response issues. It is currently prepared to offer non−credit continuing educations courses dealing with national incident management systems; terrorism and weapons of mass destruction (WMD) awareness and operations; hospital response to WMD incidents; and procedures for first responders to WMD. Additional information: http://academic.scranton.edu/department/cce/HSIHomepage.html
Source: http://matrix.scranton.edu/press/ab_press.shtml

22. *June 09, New Hampshire Union Leader* — **Disaster drill fine−tunes procedures.** City, state and federal agency representatives Wednesday, June 8, dealt with a potential disaster in downtown Manchester, NH: a leaking rail car filled with anhydrous ammonia. Turning it into a terror drill was the fact that the rail car had explosive devices under it. With about 45 participants, observers and evaluators divided among three rooms, the drill was designed to simulate the communications systems that would need to be used, with the decision−makers in the Emergency Operations Center in one room, with communications and support personnel in the others. Initially, it appeared the chemical plume would move down the river, resulting in a minimal threat to humans, but a wind shift sent it southward over residential neighborhoods. The decision was made to focus on "shelter in place." Evaluators asked why efforts wouldn't be made to evacuate residents and how people would be notified to stay indoors and seal up their homes. The responses included the difficulty in communicating because multiple languages are spoken in the affected area, as well as the numbers of people. Alerting the news media, and enlisting their help, would be one of the first steps taken, with a focus on television and radio stations.
Source: http://www.theunionleader.com/articles_showa.html?article=55 995

[Return to top]

Information Technology and Telecommunications Sector

23.

June 09, SecurityFocus — **IBM AIX GetLVName command line argument local buffer overflow vulnerability.** IBM AIX getlvname is prone to a local buffer overflow vulnerability. A buffer overflow exists in the handling of the commandline arguments to getlvname. When parsing and concatenating the supplied arguments a length parameter is not checked and a typical overflow occurs. A successful attack allows arbitrary machine code execution with super user privileges, facilitating privilege escalation. Vendor solution is pending.
Source: http://www.securityfocus.com/bid/13914/discuss

24. *June 09, SecurityFocus* — **TCPDump BGP decoding routines denial of service vulnerability.** TCPDUMP is prone to a vulnerability that may allow a remote attacker to cause a denial of service condition in the software. The issue occurs due to the way tcpdump decodes Border Gateway Protocol (BGP) packets. A remote attacker may cause the software to enter an infinite loop by sending malformed ISIS packets resulting in the software hanging. Updates are available from vendors.
Source: http://www.securityfocus.com/advisories/8671

25. *June 08, Apple* — **Mac OS X Folder permission flaw may let local users gain elevated privileges.** A vulnerability was reported in Mac OS X in the enforcement of folder permissions. A local user may be able to gain elevated privileges. A local user can exploit a race condition in assignment of permissions on files in the system's cache folder and the Dashboard system widgets. A local user may be able to write to files in those directories. See Source link below for updates.
Source: http://docs.info.apple.com/article.html?artnum=301742

26. *June 08, Reuters* — **Broadband us in Europe surpasses Americas.** More Europeans than Americans had a broadband Internet connection in the first quarter, according to a survey published Wednesday, June 8, which also showed South Korea is on the verge of losing its global pole position. The Asia Pacific region, where most of the world's population live, remained the world's biggest broadband market with 61 million subscribers and a 39 percent share of the global broadband market, Anglo−Dutch research group TelecomPaper said. Europe was second with 47.95 million fast Internet subscribers, overtaking the Americas with 47.53 million. "Europe has outrun the Americas for the first time in history and became the second largest broadband market in the world," TelecomPaper said in a note. The increase was led by countries such as the Netherlands and Denmark which are now trailing only slightly behind South Korea, where growth of Internet connections has almost come to a standstill. "Given the slow growth of South Korea, we expect that the top position, now held by South Korea, will change hands this year," said TelecomPaper director Ed Achterberg.
TelecomPaper Report Summary: http://www.telecompaper.com/reports/reportinfo.asp?id=150
Source: http://money.cnn.com/2005/06/08/news/international/broadband.reut/index.htm?cnn=yes

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT has received reports indicating an increase in the scanning for and exploitation of systems affected by one or more vulnerabilities in the Microsoft ASN.1 Library (MSASN1.DLL). These vulnerabilities are caused by the way that certain ASN.1 length values and bit strings are decoded. By sending specially crafted ASN.1 data, an attacker may be able to execute arbitrary code with SYSTEM privileges and gain complete control of a vulnerable system. MS04−007 explains how an attacker could exploit these vulnerabilities. "Because ASN.1 is a standard for many applications and devices, there are many potential attack vectors. To successfully exploit this vulnerability, an attacker must force a computer to decode malformed ASN.1 data. For example, when using authentication protocols based on ASN.1 it could be possible to construct a malformed authentication request that could expose this vulnerability." It is possible that these attacks target Secure Sockets Layer (SSL) or other cryptographic authentication capabilities in Microsoft Internet Information Server (IIS). In addition, a number of exploit tools now include functionality to take advantage of these vulnerabilities. Microsoft has released a patch to address these vulnerabilities in Microsoft Security Bulletin MS04−007.

Current Port Attacks

Top 10 Target Ports	445 (microsoft−ds), 135 (epmap), 6881 (bittorrent), 27015 (halflife), 139 (netbios−ssn), 1026 (−−−), 7845 (−−−), 4913 (−−−), 6346 (gnutella−svc), 53 (domain) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

27. *June 12, New York Times* — **Blast derails Moscow−bound train.** A bomb derailed a passenger train traveling from Chechnya to Moscow, Russia Sunday, June 12, injuring at least 15 people in what officials described as a terrorist attack. The derailed train was traveling from Chechnya to Moscow during Sunday's national holiday. The bombing came after a relative lull in attacks in Russia −− one suggesting that security officials were making progress against those behind a wave of terrorist acts culminating with the seizure of the school in Beslan last

September that left more than more than 330 people dead. There were no immediate claims of responsibility for the bombing. The bombing occurred about 7 a.m. as train No. 381 approached Uzunova, a village roughly 90 miles south of Moscow, officials cited by news agencies said. Nikolai N. Zakharov, a spokesperson for the Federal Security Service, said in televised remarks that "an improvised remote control device" was found some 50 yards from the site of the explosion. The force of the blast derailed the locomotive and four passenger wagons, but did not overturn them.
Source: http://www.nytimes.com/2005/06/12/international/europe/12cnd−russia.html?hp&ex=1118635200&en=c77ed24dbca0c9be&ei=5094&pa rtner=homepage

[Return to top]

DHS/IAIP Products & Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures:

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS/IAIP Daily Open Source Infrastructure Report is available on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

Homeland Security Advisories and Information Bulletins − DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact. Homeland Security Advisories and Information Bulletins are available on the Department of Homeland Security Website: http://www.dhs.gov/dhspublic/display?theme=70

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 983−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer

The DHS/IAIP Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.